Les bases fondamentales de la sécurité :

Superviser la position de sécurité

splunk>
turn data into doing™

La plupart des outils de cybersécurité sont conçus pour identifier et signaler un type particulier d'activité malveillante. Mais il incombe toujours à l'entreprise de déterminer si l'alerte est pertinente dans un contexte plus vaste.

Splunk facilite la centralisation de l'analyse et de la visibilité dans un environnement de sécurité multi-couches, permettant aux équipes de sécurité de déterminer rapidement si une investigation approfondie est nécessaire.

C'est la première étape d'une amélioration concrète de la planification de sécurité et de la préparation de votre entreprise, que l'on désigne comme position de sécurité.

Avec Splunk, vous pouvez obtenir rapidement des réponses aux questions les plus pressantes entourant votre position de sécurité :

- Mes points de terminaison sont-ils protégés ?
- Que se passe-t-il exactement sur mon réseau ?
- Où faut-il impérativement faire des mises à jour ?
- Les comptes utilisateurs sont-ils configurés correctement ?
- Y a-t-il un trafic sortant suspect sur notre réseau ?
- Y a-t-il des changements imprévus dans mon environnement AWS ?

Accélérez le renforcement de votre position de sécurité

Commencez par collecter et analyser l'activité des hôtes, du réseau, des antivirus et du cloud, que l'on retrouve dans tous les environnements IT ou presque.

L'activité des hôtes Windows et Linux/*nix peut révéler des problèmes potentiels de sécurité et de conformité. L'activité de connexion et les événements liés aux processus offrent un excellent point de départ.

Les logs de pare-feu, de proxy et d'e-mail peuvent fournir des renseignements critiques sur des activités de communication pouvant exiger une investigation plus approfondie, parce qu'elles évoquent par exemple un vol de propriété intellectuelle ou de données personnelles ou identifiables, une opération de commande et contrôle ou encore une tentative d'hameçonnage.

Les logs d'antivirus (AV) et de détection des points de terminaison et réponse (EDR) peuvent apporter des éclairages utiles sur les activités à l'échelle des processus, des fichiers et des utilisateurs, facilitant ainsi l'identification d'un large éventail de menaces englobant autant les virus, les malwares que les logiciels espions.

Les activités AWS inattendues et les erreurs de configuration peuvent indiquer s'il s'agit d'un problème de sécurité nécessitant une investigation (activité d'un utilisateur, modification de la topologie ou des stratégies de sécurité, utilisation de ressources, etc.).

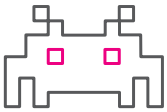
Points de départ stratégiques

Fondamentaux du réseau, de Windows, des malwares et d'AWS

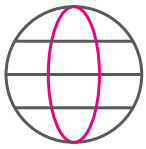
Les architectures de sécurité comprennent généralement plusieurs couches. On peut ainsi exploiter facilement ces trois couches couramment déployées afin d'obtenir des renseignements de sécurité critiques sur la position de sécurité, y compris les hôtes Windows et Linux, les pares-feux et les antivirus. Ces trois dimensions sont présentes dans pratiquement tous les environnements IT. De nombreuses entreprises utilisent également l'activité de supervision d'AWS pour obtenir de précieuses informations de sécurité sur cet environnement dans le contexte global du cloud, ainsi que sur la position de sécurité en général.

Exploitez ces quatre sources de données de base pour améliorer rapidement votre position de sécurité

Point de terminaison



Logiciels malveillants



Réseau

Cloud

Position de sécurité fondamentale de Windows et Linux

En prenant les hôtes Windows et Linux comme point de départ, l'analyse de l'activité de connexion et des événements liés aux processus peut révéler des signes précurseurs d'intentions malveillantes. L'authentification est à la base des déplacements latéraux et de l'accès aux actifs et à la propriété intellectuelle.

Connexions réussies et échecs

Les tendances identifiées dans les réussites et les échecs de connexion peuvent mettre au jour une activité inhabituelle ou malveillante (tentatives d'accès par force brute, tentatives de découverte de ressources internes ou externes), qui peut être une étape dans l'accès à un actif plus stratégique ou une tentative de prise de contrôle administratif.

Connexions à de nouveaux comptes

Les connexions inattendues à de « nouveaux comptes » et les « premières connexions » peuvent être le symptôme d'une exploitation d'identifiants privilégiés ou d'un partage d'identifiants.

Connexions anormales

Une activité anormale peut se traduire par un nombre supérieur à la moyenne de tentatives de connexion, un pic temporaire de connexions à de nombreux actifs depuis un même compte, ou des tentatives de connexion provenant simultanément de plusieurs régions différentes. Ces activités trahissent potentiellement le partage ou l'exploitation non autorisés d'identifiants ou bien un compte compromis.

Nouveaux processus

Une fois qu'un accès non autorisé à un hôte a eu lieu – ou qu'un malware s'est installé, apparaissent de nouveaux processus à l'aspect légitime. On peut observer de faux processus système qui semblent émaner du système d'exploitation et échappent ainsi aux mécanismes traditionnels de détection en se cachant derrière un nom de fichier ou une signature « légitime ».

Position de sécurité fondamentale du réseau

Le réseau est un domaine critique qui vous informe sur l'entretien et l'amélioration de la position de sécurité, car toutes les communications entre les machines, les applications et les utilisateurs passent par le réseau. Les données de pare-feu, notamment, peuvent délivrer des renseignements stratégiques sur les tendances de communication pouvant signaler des problèmes de sécurité à explorer ou corriger, comme le vol de propriété intellectuelle ou la communication avec un serveur de commande et contrôle.

Applications consommant le plus de bande passante

Les applications qui enregistrent un changement brutal dans la quantité de bande passante consommée peuvent être compromises. La cause profonde du phénomène peut être une exfiltration de données ou une activité de commande et contrôle en relation avec un hôte malveillant connu.

Classement par utilisation des protocoles

Il est intéressant de savoir si l'utilisation des protocoles dépasse les valeurs attendues, par exemple si un trafic important est dirigé vers un réseau TOR ou si du trafic SMB quitte le réseau de l'entreprise. Ce trafic peut être causé par un malware en train d'établir un canal de commande et contrôle ou de tenter de télécharger des composants malveillants supplémentaires tels que des modules de chiffrement de ransomware.

Classement par consommation de bande passante

Des modifications de la consommation de bande passante peuvent être le signe d'une exfiltration de données ou autre activité non autorisée telle que la livraison de malwares.

Classement des exécutables bloqués

Des variantes peuvent passer inaperçues si elles ne correspondent pas à une signature, une valeur de hachage ou un nom de fichier – du moins jusqu'à leur détonation dans une sandbox. Cet indicateur fournit du contexte sur les familles de malwares les plus couramment déployés dans une campagne d'hameçonnage ou d'infection, ainsi que des renseignements sur le comportement des tentatives d'infection qui s'ensuivent.

Position de sécurité fondamentale face aux malwares

Les solutions antivirus offrent des renseignements stratégiques sur les activités à l'échelle des processus, des fichiers et des utilisateurs, notamment en fournissant des informations au niveau du système et des hôtes : sur les processus, le réseau et les fichiers mais aussi, selon la solution, sur toute une gamme de types de menaces englobant virus, malwares, logiciels espions, listes blanches et même preuves comportementales. Le point de terminaison offre une base de collecte et de lancement pour la plupart des infections basées sur un malware. Il constitue donc une source de données cruciale qui doit être considérée comme fondamentale pour renforcer immédiatement la position de sécurité.

Classement des risques détectés

L'antivirus peut calculer les risques associés à des vulnérabilités spécifiques et leurs exploitations connues, et cette métrique peut orienter la hiérarchisation du traitement de grands volumes d'événements suspects et anormaux.

Classement des processus bloqués

Bénéficier d'une visibilité complète sur les applications connues et inconnues est crucial pour la méthodologie appliquée aux points de terminaison. Cette métrique délivre des renseignements approfondis sur les activités malveillantes et leur signification, en particulier lorsqu'elles sont envisagées dans le contexte de leur fréquence, du moment où elles surviennent, des utilisateurs et autres paramètres pouvant permettre de déterminer si le problème rencontré est plus vaste – une campagne d'hameçonnage ciblé par exemple.

Classement des virus et logiciels espions détectés

il est toujours essentiel d'exclure les virus et les logiciels espions, en particulier dans les environnements qui emploient des systèmes d'exploitation anciens, en fin de prise en charge, et pour lesquels il n'existe plus de correctifs. De plus, de nouveaux malwares exploitant les mécanismes d'anciennes souches de virus et de logiciels espions continuent d'évoluer et restent utilisés dans des opérations de reconnaissance ou de livraison. C'est notamment le cas des ransomwares et des applicatifs de minage de Bitcoin.

Rapports de version des clients anti-malware

C'est une métrique cruciale non seulement en termes de protection, mais aussi pour le respect des obligations de conformité et autres exigences réglementaires.

Rapports de version des définitions de virus

Il est impératif de savoir si les points de terminaison ont reçu les mises à jour des définitions de virus pour assurer votre conformité et empêcher la propagation des infections non traitées ainsi que la réinfection des hôtes nettoyés par les mêmes virus.

Définition de la position de sécurité

Position de sécurité fondamentale d'AWS

La supervision et la visibilité en temps réel du cloud ou de votre environnement multicloud peut apporter des renseignements de sécurité d'une grande valeur. Qu'elles abritent un seul service ou des centaines, les solutions et infrastructures cloud créent plusieurs difficultés malgré leurs nombreux avantages. L'incapacité à superviser et contrôler les données qui entrent et sortent du cloud peuvent avoir de sévères répercussions en aval. Dans ce contexte, une visibilité en temps réel sur votre environnement AWS représente un atout de poids. Des modifications inattendues des ACL du réseau, les groupes de sécurité, l'activité IAM ou S3 peuvent être le signe d'un problème de sécurité à explorer.

Groupes de sécurité

Les groupes de sécurité jouent le rôle de pare-feu en contrôlant le trafic entrant et sortant des instances EC2 déployées au sein d'un VPC. La supervision de l'activité des groupes de sécurité et la détection des changements inhabituels ou inattendus peuvent délivrer des renseignements de sécurité stratégiques. Par exemple, un changement soudain du nombre de règles de groupes de sécurité peut trahir un problème méritant votre attention.

ACL réseau

Les ACL réseau constituent une couche de sécurité optionnelle et peuvent offrir des renseignements de sécurité de haut niveau sur la circulation du trafic à destination et en provenance des sous-réseaux VPN. Un changement soudain du nombre de modifications des ACL indique souvent un problème à explorer.

Activité IAM

La supervision de l'activité IAM permet de déterminer si la façon dont les utilisateurs accèdent aux services et aux ressources AWS est problématique. Elle permet ainsi de repérer un pic de tentatives non autorisées touchant des actions spécifiques comme la création ou la suppression de clés d'accès ou de comptes utilisateurs.

Buckets S3

Supervisez les buckets S3 pour vous assurer qu'ils sont correctement configurés : en particulier, ils ne doivent pas être accessibles publiquement.

Mise en œuvre des techniques de supervision fondamentales dans Splunk

Voici quelques techniques simples à appliquer dans Splunk pour prendre un bon départ :

Détection de base des attaques par force brute

La découverte des identifiants d'un utilisateur est une stratégie essentielle de l'adversaire. Une technique courante consiste à deviner un mot de passe faible en essayant des centaines de mots de passe fréquemment employés. Comme la plupart des environnements utilisent Active Directory comme référentiel centralisé d'identifiants, toute stratégie de sécurité doit absolument inclure la recherche des attaques par force brute dans les logs de sécurité Windows.

Source(s) de données : Sécurité Windows

Ce que vous devez rechercher : Les échecs de connexion émanant d'une source donnée, et suivis d'une connexion réussie provenant de la même source.

Balayage de base

Le balayage permet aux adversaires de découvrir la surface d'attaque du réseau d'une entreprise. Il devrait être exclusivement le fait de sources autorisées (détecteurs de vulnérabilités, par exemple). Si un autre agent balaye votre réseau, vous devez impérativement procéder à une vérification et une investigation approfondie.

Source(s) de données : Pares-feux, proxys

Ce que vous devez rechercher : Les hôtes cherchant à atteindre de nombreux hôtes ou ports sur une courte période.

Connexion réussie d'un ancien employé

Généralement, les comptes utilisateurs des anciens employés ne doivent enregistrer aucune activité après leur départ de l'entreprise. Si une connexion a lieu après leur départ, cela peut signifier que leurs identifiants ont été compromis ou qu'ils tentent de se connecter pour réaliser des opérations non autorisées.

Source(s) de données : Authentification, sécurité Windows

Ce que vous devez rechercher : Toute activité de connexion au compte utilisateur d'un ancien employé.

Envoi massif de données sur le web

L'exfiltration de données se produit généralement via des canaux standards : les utilisateurs envoient les données vers Google, Dropbox, Box, de petits sites de partage de fichiers, voir des sites de dépôt non référencés. Comme les sessions HTTPS sortantes sont souvent autorisées, l'exfiltration de données devient relativement facile dans la plupart des entreprises.

Source(s) de données : Proxy web

Ce que vous devez rechercher : Les envois dépassant un certain seuil vers des applications cloud spécifiques.

Bucket S3 public dans AWS

Les buckets S3 ouverts sont couramment exploités dans les failles de données. Les fichiers hébergés qui devraient être supprimés ne le sont pas, ou bien les permissions sont mal configurées sur des buckets S3 utilisés pour sauvegarder des données sensibles. Les nouveaux buckets S3 sont supervisés et les données en sont rapidement extraites. Il s'agit d'une méthodologie de base pour tout environnement AWS d'entreprise ; la supervision et l'analyse des buckets S3 ouverts doivent être des priorités.

Source(s) de données : Suivi d'audit

Ce que vous devez rechercher : Tout bucket S3 configuré pour être accessible publiquement ainsi que toute activité associée.

Réponse de base aux attaques de malware

Lorsque le même malware apparaît sur plusieurs systèmes, cela peut être le signe que votre entreprise est à l'aube d'un incident majeur (on l'a souvent vu avec les vers, les ransomware et les grandes campagnes d'hameçonnage).

Source(s) de données : Antivirus

Ce que vous devez rechercher : Les apparitions de malwares identiques sur plusieurs systèmes et sur une courte période.

Désactivation du service Windows Update

La maintenance des correctifs est un aspect essentiel d'une cyber-hygiène efficace. Les systèmes Windows sont particulièrement exposés lorsqu'ils ne sont pas à jour, étant donné le nombre et la fréquence des exploitations qui ciblent les vulnérabilités de Windows pour s'implanter, se déplacer latéralement ou se propager.

Les systèmes Windows qui cessent de se mettre à jour peuvent être la cible d'activités malveillantes, mais ce problème peut aussi provenir d'une modification de l'environnement, d'un défaut de configuration ou d'un arrêt planifié. Si le service de mise à jour lui-même est désactivé sur l'hôte, cela peut indiquer une compromission.

Source(s) de données : Événements Windows

Ce que vous devez rechercher : Les systèmes Windows dont le service Windows Update est désactivé.

Infections multiples sur un hôte

Une infection par plusieurs virus simultanément est plus inquiétante car elle peut trahir la présence d'un kit d'exploitation en train d'essayer plusieurs techniques pour optimiser ses chances de réussite, ou signaler un hôte présentant plusieurs vulnérabilités indépendantes les unes des autres. Ces hôtes doivent être traités en priorité et explorés sans délai afin d'identifier d'autres éléments qui n'auraient pas été détectés.

Source(s) de données : Antivirus

Ce que vous devez rechercher : Les hôtes qui ont enregistré plusieurs infections différentes sur une période courte.

Faux processus Windows

Les malwares et autres activités malveillantes tentent souvent de se dissimuler, notamment en prenant la forme de processus légitimes. Les processus malveillants sont généralement exécutés depuis des emplacements atypiques, plutôt que des répertoires système habituels tels que Windows\System32 ou Windows\SysWOW64.

Source(s) de données : Détection des points de terminaison et réponse, Sécurité Windows

Ce que vous devez rechercher : Les processus présentant un nom légitime et qui s'exécutent normalement à partir de Windows\System32 ou Windows\SysWOW64, mais s'exécutent ici depuis un autre emplacement. Par exemple, les ransomwares créent souvent des processus qui se cachent derrière des noms de processus légitimes mais s'exécutent dans des emplacements inhabituels comme le Bureau ou le répertoire \temp.

E-mails provenant de domaines ressemblants

L'envoi d'e-mails provenant d'un nom de domaine similaire à un domaine légitime est une technique d'hameçonnage courante. Un e-mail peut ainsi être envoyé par une adresse en @spiunk.com plutôt que @splunk.com.

Source(s) de données : E-mail

Ce que vous devez rechercher : Les e-mails provenant de domaines similaires à ceux de votre entreprise, avec une légère variante (comme une lettre manquante ou une faute d'orthographe).

Nouveau compte d'administration local

Les comptes d'administration locaux sont souvent employés par les pirates. Cette méthode détecte les comptes récemment créés et élevés à un niveau supérieur de privilèges.

Source(s) de données : Suivi d'audit, sécurité Windows

Ce que vous devez rechercher : Les comptes récemment créés avec des privilèges d'administrateur local.

Commencez dès maintenant à renforcer votre position de sécurité

Splunk vous permet d'exercer un contrôle plus étroit sur la position de sécurité de votre entreprise, pour que vous obteniez plus rapidement des réponses et des informations, notamment sur les causes profondes d'une attaque et de son impact.

Obtenez rapidement la visibilité dont vous avez besoin pour évaluer votre position et ainsi normaliser vos investigations afin de prendre des décisions de sécurité plus efficaces, plus rapides et plus précises.

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

AW-20-13315-SPLK-Essential-security-foundations-106-WP